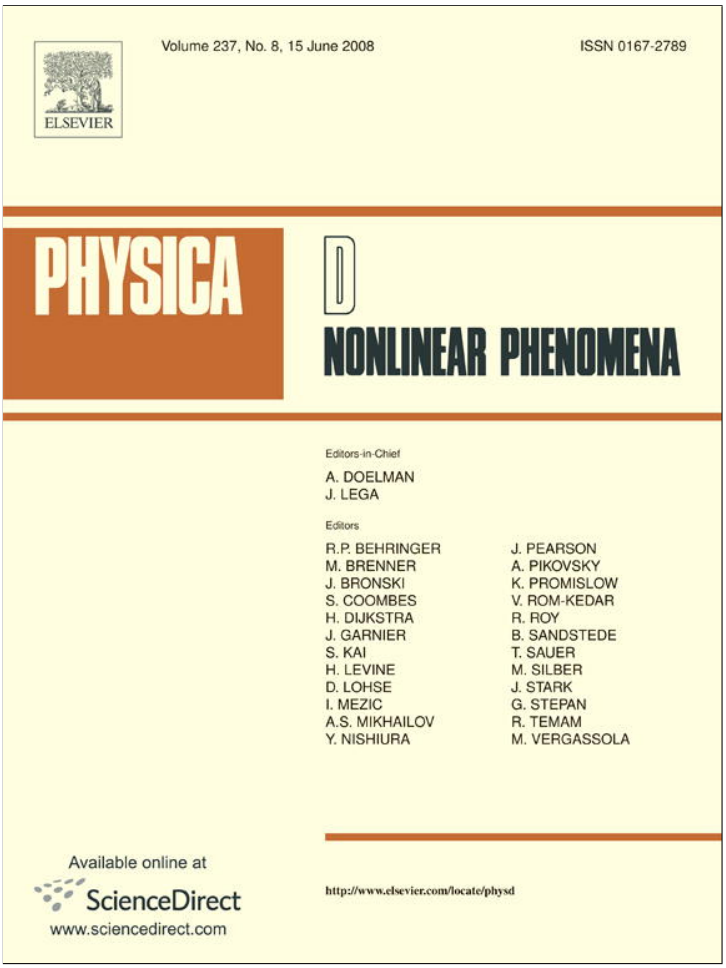

Available online at www.sciencedirect.com
ScienceDirect
Physica D 237 (2008) 1074–1078
PHYSICA D
www.elsevier.com/locate/physd

Enhanced quantum searching via entanglement and partial diffusion

A. Younes[a,*], J. Rowe[b], J. Miller[c]

[a] Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Alexandria, Egypt
[b] School of Computer Science, University of Birmingham, Birmingham, Edgbaston, B15 2TT, United Kingdom
[c] Department of Electronics, University of York, York, Heslington, YO10 5DD, United Kingdom

Received 19 May 2007; accepted 19 December 2007
Available online 31 December 2007

Communicated by S. Kai

Abstract

In this paper, we will define a quantum operator that performs the standard inversion about the mean only on a subspace of the system (*Partial Diffusion Operator*). This operator is used together with entanglement in a quantum search algorithm that runs in $O(\sqrt{N/M})$ for searching an unstructured list of size N with M matches such that $1 \leq M \leq N$. We will show that the performance of the algorithm is more reliable than known *fixed operators quantum search algorithms* especially for multiple matches where we can get a solution after a single iteration with probability over 90% if the number of matches is approximately more than one-third of the search space. We will show that the algorithm will be able to handle the case where the number of matches M is unknown in advance in $O(\sqrt{N/M})$ such that $1 \leq M \leq N$.

PACS: 03.67.Lx

Keywords: Quantum search; Amplitude amplification; Entanglement

1. Introduction

In 1996, Grover [5] presented a quantum search algorithm for a single match within an unstructured list of N items with quadratic speed-up over classical algorithms. Much work has been done to analyze and/or generalize the algorithm for multiple matches [2,4] where it was shown that the number of iterations is approximately $\pi/4\sqrt{N/M}$ for small M/N, where M is the number of matches, to get a probability of success at least 50% when $M/N = 0.5$. It was shown in [8] that the problem will be harder for multiple matches where it might be expected to be easier. Other work has been done for a known number of multiple matches with arbitrary superposition and phase shifts [1,3,7]. For the sake of practicality, the operators should be fixed and are able to handle the problem with high probability whether or not M is known in advance. In this paper, we will propose a quantum algorithm that uses fixed amplitude amplification operators that runs in $O(\sqrt{N/M})$. The algorithm gives higher probability of success than known quantum search algorithms where it needs only *a single iteration* to get probability over 90% if $M/N > 1/3$ and with probability of success at least 87.88% over the whole range. In [10] Younes et al. presented an algorithm that exploits entanglement and uses partial diffusion operator to perform the quantum search. Grover described this algorithm as the best quantum search algorithm [6].

In this paper, we will extend [10] to show that algorithm is able to handle the whole range $1 \leq M \leq N$ more reliably whether or not the number of matches is known in advance. The plan of the paper is as follows: Section 2 introduces the general definition of the unstructured search problem. Section 3 defines the partial diffusion operator. Section 4 introduces the algorithm and an analysis of its behavior. Section 5 shows a comparison with Grover's original algorithm. Section 6 introduces the algorithm shown in [2] for an unknown number of matches by replacing Grover's algorithm with the algorithm proposed here. The paper will end up with a general conclusion in Section 7.

* Corresponding author. Tel.: +20 101368289.
E-mail addresses: ayounes2@yahoo.com (A. Younes), J.E.Rowe@cs.bham.ac.uk (J. Rowe), jfm@ohm.york.ac.uk (J. Miller).

0167-2789/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.physd.2007.12.005

2. Unstructured search problem

Consider an unstructured list L of N items such that $L = \{0, 1, \ldots, N-1\}$. For simplicity and without loss of generality we will assume that $N = 2^n$ for some positive integer n. Consider a function (oracle) f which maps an item $i \in L$ to either 0 or 1 according to some properties this item should satisfy, i.e. $f : L \to \{0, 1\}$. The problem is to find any $i \in L$ such that $f(i) = 1$ assuming that such an i exists in the list.

3. Partial diffusion

The *partial diffusion operator*, P_{inv}, is an operator which performs the inversion about the mean, and a phase shift of -1 on the *subspace* of the system entangled with the extra qubit workspace in state $|0\rangle$, and $|1\rangle$ respectively. The diagonal representation of P_{inv} when applied on $n+1$ qubits system can take this form:

$$P_{inv} = \left(H^{\otimes n} \otimes I_1\right)\left(2\,|0\rangle\,\langle 0| - I_{n+1}\right)\left(H^{\otimes n} \otimes I_1\right), \tag{1}$$

where the vector $|0\rangle$ used in Eq. (1) is of length 2^{n+1}, H is the Hadamard gate $\left(H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)$, and I_k is the identity matrix of size $2^k \times 2^k$. A general quantum system of size $n+1$ can be represented as follows:

$$|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j \left(|j\rangle \otimes |0\rangle\right) + \sum_{j=0}^{N-1} \beta_j \left(|j\rangle \otimes |1\rangle\right). \tag{2}$$

Applying P_{inv} on $|\psi\rangle$ gives,

$$\sum_{j=0}^{N-1} \left(2\,\langle\alpha\rangle - \alpha_j\right)\left(|j\rangle \otimes |0\rangle\right) - \sum_{j=0}^{N-1} \beta_j \left(|j\rangle \otimes |1\rangle\right), \tag{3}$$

where $\langle\alpha\rangle = \frac{1}{N}\sum_{j=0}^{N-1} \alpha_j$ represents the mean of the amplitudes of the subspace $\sum_{j=0}^{N-1} \alpha_j \left(|j\rangle \otimes |0\rangle\right)$, i.e. applying the operator P_{inv} will perform the inversion about the mean only on the subspace $\sum_{j=0}^{N-1} \alpha_j \left(|j\rangle \otimes |0\rangle\right)$ and will only change the sign of the amplitudes for the rest of the system, i.e. $\sum_{j=0}^{N-1} \beta_j \left(|j\rangle \otimes |1\rangle\right)$.

4. The algorithm

For a list of size $N = 2^n$, prepare a quantum register of size $n+1$ qubits all in state $|0\rangle$ and apply the steps of the algorithm as follows. Its quantum circuit is shown in Fig. 1:

1- Apply the Hadamard gate on each of the first n qubits so they contain the 2^n values representing the list.
2- Iterate the following steps q times:
   i- Apply the oracle U_f to map the items in the list to either 0 or 1 simultaneously and store the result in the extra workspace qubit,
   $U_f\,|x, 0\rangle \to |x, f(x)\rangle$.
   ii- Apply the partial diffusion operator P_{inv}.
3- Measure the first n qubits.

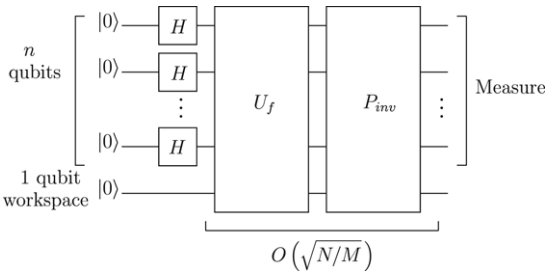

Fig. 1. Quantum circuit for the proposed algorithm.

4.1. Analysis of performance

The main idea of using the partial diffusion is to split the subspace of the solutions into two smaller subspaces [10]. In each iteration, one of the solution subspaces will be inverted about the mean (together with the non-solution subspace) while the other half will have the sign of their amplitudes changed to the negative sign, preparing it to be inverted about the mean (together again with the non-solution subspace) in the next iteration. The benefit of this alternating inversion is to preserve half the number of the solution states at each iteration so as to resist the *de-amplification behavior* of the standard diffusion operator when reaching the so-called turning points. The oracle U_f will create *entanglement* between the solution and non-solution subspaces and the extra working qubit after the first iteration. Applying U_f afterwards will *swap* the two solution subspaces by switching the entanglement without affecting the non-solution sub-space.

Let M be the number of matches, which makes the oracle f evaluates to 1, such that $1 \le M \le N$. Assume that $\sum_i'$ indicates a sum over all i which are desired matches, and $\sum_i''$ indicates a sum over all i which are undesired items in the list. The system after $q \ge 2$ iterations can be expressed as follows:

$$\left|W^{(q)}\right\rangle = a_q \sum_{i=0}^{N-1}{}'' \left(|i\rangle \otimes |0\rangle\right) + b_q \sum_{i=0}^{N-1}{}' \left(|i\rangle \otimes |0\rangle\right) + c_q \sum_{i=0}^{N-1}{}' \left(|i\rangle \otimes |1\rangle\right), \tag{4}$$

such that,

$$(M-N)a_q^2 + M(b_q^2 + c_q^2) = 1, \tag{5}$$

notice that we are dealing mathematically with the whole $n+1$ qubits system including the extra qubit workspace. The mean to be used in the definition of P_{inv} is as follows: Let $y = 1 - M/N$ and $s = 1/\sqrt{N}$, then $\langle\alpha_q\rangle = y a_{q-1} + (1-y)c_{q-1}$, and a_q, b_q and c_q used in Eq. (4) are calculated as follows:

$$\begin{aligned} &a_0 = s, \quad a_1 = s\,(2y-1), \quad a_q = 2\langle\alpha_q\rangle - a_{q-1},\\ &b_0 = s, \quad b_1 = 2sy, \quad b_q = 2\langle\alpha_q\rangle - c_{q-1},\\ &c_0 = 0, \quad c_1 = -s, \quad c_q = -b_{q-1}. \end{aligned} \tag{6}$$

The probabilities of the system to find a solution $P_s^{(q)}$ and not to find a solution $P_{ns}^{(q)}$ are,

$$P_s^{(q)} = M(b_q^2 + c_q^2), \qquad P_{ns}^{(q)} = (N-M)\,a_q^2, \tag{7}$$

notice that, using Eq. (5), $P_s^{(q)} + P_{ns}^{(q)} = 1$. Solving the above recurrence relations shown in Eq. (6), the closed forms are as follows:

$$a_q = s\left(U_q(y) - U_{q-1}(y)\right), \quad b_q = sU_q(y), \quad c_q = -sU_{q-1}(y), \tag{8}$$

where $U_q(y) = \sin((q+1)\theta)/\sin(\theta)$ is the Chebyshev polynomial of the second kind [9], $y = \cos(\theta) = 1 - M/N$ and $0 < \theta \leq \pi/2$.

To find a match with probability as close as possible to certainty on any measurement, we have to find $\overline{q}$ such that $P_s^{(\overline{q})} = 1$, this will happen when $\overline{q} = \pi/2\theta - 1/2$. The number of iterations must be an integer, let $q = \lfloor \pi/2\theta \rfloor$ where $|q - \overline{q}| \leq 1/2$ and $\lfloor\ \rfloor$ is the floor operation. Since, $\cos(\theta) = 1 - M/N$, we have $\theta \geq \sin(\theta) = \sqrt{2NM - M^2}/N$, then,

$$q = \left\lfloor \frac{\pi}{2\theta} \right\rfloor \leq \frac{\pi}{2\theta} \leq \frac{\pi}{2\sqrt{2}}\sqrt{\frac{N}{M}} = O\left(\sqrt{\frac{N}{M}}\right), \tag{9}$$

where the lower bound of $P_s^{(q)}$ using q shown in Eq. (9) is given by,

$$P_s^{(q)} \geq \frac{1 + \cos^2(\theta)}{1 + \cos(\theta)} = \frac{1 + \left(1 - \frac{M}{N}\right)^2}{1 + \left(1 - \frac{M}{N}\right)} \geq 0.828. \tag{10}$$

5. Unknown number of matches

In case we do not know the number of matches M in advance, we can apply the algorithm shown in [2] for $1 \leq M \leq N$ by replacing Grover's algorithm with the proposed algorithm. The algorithm can be summarized as follows:

1- Start with $m = 1$ and $\lambda = 8/7$. (where λ can take any value between 1 and 4/3).
2- Pick an integer j between 0 and $m - 1$ in a uniform random manner.
3- Run j iterations of the proposed algorithm on the state:

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle.$$

4- Measure the register and assume that i is the output.
5- If $f(i) = 1$, then we found a solution and exit.
6- Let $m = min\left(\lambda m, \sqrt{N}\right)$ and go to step 2.

For the sake of simplicity and to be able to compare the performance of this algorithm with that shown in [2], we will try to follow the same style of analysis used in [2]. Before we construct the analysis, we need the following lemmas. The first lemma is straightforward using mathematical induction.

Lemma 5.1. *For any positive integer m and real number θ such that* $0 < \theta \leq \pi/2$,

$$\sum_{q=0}^{m-1} \sin^2((q+1)\theta) + \sin^2(q\theta) = m - \frac{\cos(\theta)\sin(2m\theta)}{2\sin(\theta)}.$$

Lemma 5.2. *Assume that M is the unknown number of matches such that* $1 \leq M \leq N$. *Let θ be a real number such that* $\cos(\theta) = 1 - M/N$ *and* $0 < \theta \leq \pi/2$. *Let m be any positive integer. Let q be any integer picked in a uniform random manner between 0 and* $m - 1$. *Measuring the register after applying q iterations of the proposed algorithm starting from the initial state, the probability* P_m *of finding a solution is as follows,*

$$P_m = \frac{1}{1 + \cos(\theta)}\left(1 - \frac{\cos(\theta)\sin(2m\theta)}{2m\sin(\theta)}\right),$$

where, $P_m \geq 0.2725$ *for* $m \geq 1/\sin(\theta)$.

Proof. Using Eqs. (7) and (8), the probability of success when applying $\overline{q}$ iterations of the proposed algorithm

$$P_s^{(\overline{q})} = (1 - \cos(\theta))\left(\frac{\sin^2((\overline{q}+1)\theta)}{\sin^2(\theta)} + \frac{\sin^2(\overline{q}\theta)}{\sin^2(\theta)}\right).$$

The average probability of success when applying q iterations of the proposed algorithm when $0 \leq q \leq m$ is picked in a uniform random manner is as follows,

$$\begin{aligned} P_m &= \sum_{q=0}^{m-1} \frac{1}{m} P_s^{(q)} \\ &= \frac{1}{m(1 + \cos(\theta))} \sum_{q=0}^{m-1} \sin^2((q+1)\theta) + \sin^2(q\theta) \\ &= \frac{1}{1 + \cos(\theta)}\left(1 - \frac{\cos(\theta)\sin(2m\theta)}{2m\sin(\theta)}\right). \end{aligned}$$

If $m \geq 1/\sin(\theta)$ then $\cos(\theta) \approx 1$, so,

$$P_m > \frac{1}{2} - \frac{\sin(2m\theta)}{4m\sin(\theta)} \geq \frac{1}{2} - \frac{\sin(2m\theta)}{4},$$

where $\sin(2m\theta) < 0.91$ for $0 < \theta \leq \pi/2$. P_m will be at least 0.2725 when $M \ll N$, i.e. $P_m \geq 0.2725$ for $1 \leq M \leq N$. □

We calculate the total expected number of iterations following Theorem 3 in [2] to be able to compare results. Assume that $m_q \geq 1/\sin(\theta)$, and $v_q = \lceil \log_\lambda m_q \rceil$. Notice that, $m_q = O\left(\sqrt{N/M}\right)$ for $1 \leq M \leq N$, then:

1- The total expected number of iterations to reach the critical stage, i.e. when $m \geq m_q$:

$$\frac{1}{2}\sum_{v=1}^{v_q} \lambda^{v-1} < \frac{1}{2(\lambda - 1)} m_q = 3.5 m_q.$$

2- The total expected number of iterations after reaching the critical stage:

$$\frac{1}{2}\sum_{u=0}^{\infty} (0.7275)^u \lambda^{v_q + u} < \frac{1}{2(1 - 0.7275\lambda)} m_q = 2.9 m_q.$$

The total expected number of iterations whether we reach to the critical stage or not is $6.4 m_q$ which is in $O(\sqrt{N/M})$ for $1 \leq M \leq N$.

When this algorithm employed Grover's algorithm [2], and based on the condition $m_G \geq 1/\sin(2\theta_G) = O\left(\sqrt{N/M}\right)$

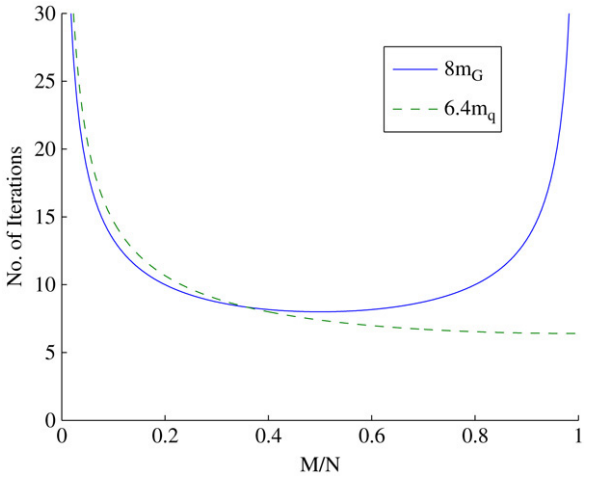

Fig. 2. The actual behavior of the functions representing the total expected number of iterations for Grover's algorithm $8m_G$ and the proposed algorithm $6.4m_q$ taking $\lambda = 8/7$, where the number of iterations is the flooring of the values (step function).

for $1 \leq M \leq 3N/4$, where m_G will act as a lower bound for q_G in that range. The total expected number of iterations is approximately $8m_G$. For $M > 3N/4$, m_G will increase exponentially where it will not be able to approximate q_G. Employing the proposed algorithm instead, and based on the condition $m_q \geq 1/\sin(\theta) = O\left(\sqrt{N/M}\right)$ for $1 \leq M \leq N$, the total expected number of iterations is approximately $6.4m_q$, i.e. the algorithm will be able to handle the whole range, since m_q will be able to act as a lower bound for q over $1 \leq M \leq N$. Fig. 2 compares between the total expected number of iterations for both algorithms taking $\lambda = 8/7$.

6. Conclusion

The probability of success of Grover's algorithm (Fig. 3) as shown in [2] is $P_s^{(q_G)} = \sin^2((2q_G + 1)\theta_G)$, where $\sin^2(\theta_G) = M/N, 0 < \theta_G \leq \pi/2$, the required number of iterations is $q_G = \lfloor \pi/4\theta_G \rfloor \leq \pi/4\sqrt{N/M}$. The lower bound of the probability of success using q_G is given by, $P_s^{(q_G)} \geq 1 - M/N \geq 0$.

In Grover's algorithm, the search space is split into two subspaces (the solution and non-solution subspaces) then amplifies the amplitudes of the solution states by iterating the diffusion operator and the oracle [5] to find a match with high probability in $O(\sqrt{N/M})$ for small M/N and in the neighborhood of $M/N = 1/4$ [2]. The main idea of using partial diffusion in quantum search is to split the subspace of the solutions into two smaller subspaces. In each iteration, one of the solution subspaces will be inverted about the mean (together with the non-solution subspace) while the other half will have the sign of their amplitudes changed to the negative sign, preparing it to be inverted about the mean (together again with the non-solution subspace) in the next iteration via entanglement. The benefit of this alternating inversion is to preserve half the number of the solution states at each iteration so as to resist the *de-amplification behavior* of the standard diffusion operator when reaching the so-called turning points and get the solution with high probability in $O(\sqrt{N/M})$ for $1 \leq M \leq N$. Apply the oracle U_f each iteration will switch the entanglement of the two solution subspaces with the extra qubit workspace to decide which subspace to be inverted about the mean with the non-solution subspace.

An algorithm for unknown number of matches replacing Grover's step in the algorithm shown in [2] is presented, where we showed that the algorithm will be able to handle the range $1 \leq M \leq N$ in $O(\sqrt{N/M})$ compared with $1 \leq M \leq 3N/4$ when using Grover's algorithm.

We showed that the algorithm will be able to handle the whole possible range $1 \leq M \leq N$ more reliably using fixed operators in $O\left(\sqrt{N/M}\right)$ for both known (as shown in Fig. 3) and unknown number of matches.

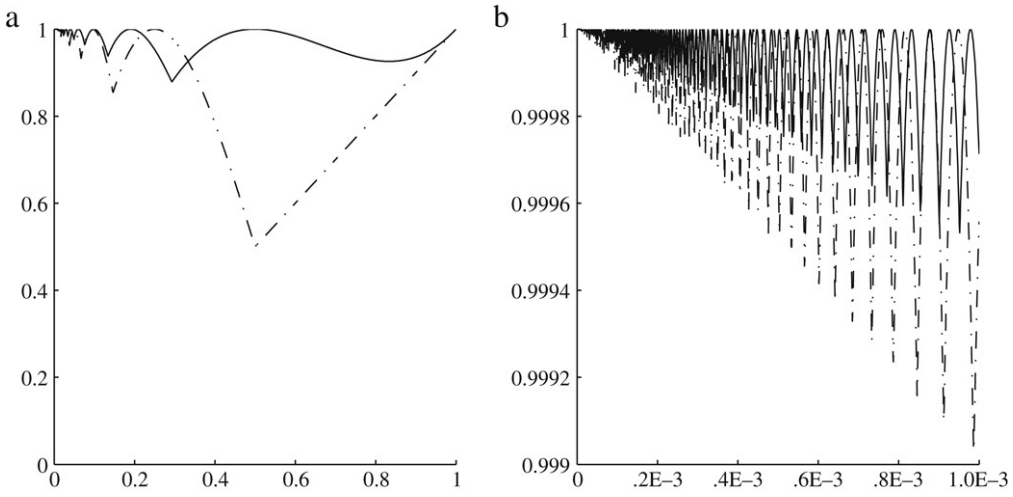

Fig. 3. Probability of success for: (a) Using the required number of iterations for both algorithms, (b) same as (a) for $M/N \leq 1 \times 10^{-3}$. *x-axis* is M/N and *y-axis* is the probability. Figures numbered from left to right and *dotted line* indicates Grover's algorithm, *solid line* indicates the proposed algorithm.

References

[1] D. Biron, O. Biham, E. Biham, M. Grassl, D.A. Lidar, quant-ph/9801066.
[2] M. Boyer, G. Brassard, P. Høyer, A. Tapp, Fortschr. Physik 46 (1998) 493.
[3] G. Brassard, P. Høyer, M. Mosca, A. Tapp, quant-ph/0005055.
[4] G. Chen, S. Fulling, M. Scully, quant-ph/9909040.
[5] L. Grover, A fast quantum mechanical algorithm for database search, in: Proc. of the 28th Ann. ACM Symp. on the Theory of Computing, 1996, pp. 212–219.
[6] L. Grover, Phys. Rev. Lett. 95 (2005) 150501.
[7] P. Høyer, Phys. Rev. A 62 (2000) 52304.
[8] M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, United Kingdom, 2000.
[9] T. Rivlin, Chebyshev Polynomials, Wiley, New York, 1990.
[10] A. Younes, J. Rowe, J. Miller, Quantum search algorithm with more reliable behaviour using partial diffusion, in: Proc. of the 7th Int. Conf. on Quantum Communication, Measurement and Computing, 2004, pp. 171–174.